

An intuitive proof of the data processing inequality

Normand J. Beaudry¹ and Renato Renner¹

¹*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

(Dated: July 6, 2011)

The data processing inequality (DPI) is a fundamental feature of information theory. Informally it states that you cannot increase the information content of a quantum system by acting on it with a local physical operation. When the smooth min-entropy is used as the relevant information measure, then the DPI follows immediately from the definition of the entropy. The DPI for the von Neumann entropy is then obtained by specializing the DPI for the smooth min-entropy by using the quantum asymptotic equipartition property (QAEF). We provide a new, simplified proof of the QAEF and therefore obtain a self-contained proof of the DPI for the von Neumann entropy.

1. INTRODUCTION

The data processing inequality (DPI) has an intuitive interpretation: the information content contained in a quantum system cannot increase by performing local data processing on that system. It is an extremely useful property that is used extensively in quantum information [1]. The DPI has been known to hold for different entropy measures, including an important quantity: the von Neumann entropy [2]. The DPI is typically stated for the case where the local operation is a partial trace, but this can be generalized to any physical operation.¹ Formally it is

$$H(A|BC)_\rho \leq H(A|B)_\rho, \quad (1)$$

where the conditional von Neumann entropy $H(A|B)$ is the uncertainty about the system A given the system B . It is defined on a normalized state in the Hilbert space \mathcal{H}_{AB} , $\rho_{AB} \in S_=(\mathcal{H}_{AB})$, as $H(A|B)_\rho := H(AB)_\rho - H(B)_\rho$, where $H(A)_\rho := -\text{Tr}(\rho \log \rho)$ (all logarithms are taken to the base 2). Also, Eqn. 1 is equivalent to the strong subadditivity of the von Neumann entropy: $H(ABC)_\rho + H(B)_\rho \leq H(AB)_\rho + H(BC)_\rho$.

The first proofs of this property relied on abstract operator properties [3–5]. Recently, these proofs have been simplified [6–8]. Other approaches have used the operational meaning of the von Neumann entropy [9, 10], Minkowski inequalities [11, 12], or holographic gravity theory [13, 14]. There has also been recent interest in the structure of states where there is equality in the DPI [15–17]. Our approach provides a new perspective by decomposing the proof of the DPI into a simple proof of a more fundamental property, followed by a specialization. It also provides a new approach to teaching the DPI.

In this paper we first prove the DPI for a different entropy: the smooth min-entropy (Theorem 1). This inequality follows directly from the partial trace applied to

the definition of the smooth min-entropy [18]. Then we can specialize the smooth min-entropy to the von Neumann entropy by the quantum asymptotic equipartition property (QAEF) (Theorem 2) [19]. However, here we provide a simpler proof to that of [19] so that we have a self-contained proof for the von Neumann entropy DPI (Theorem 3).

2. SMOOTH MIN-ENTROPY

It has become apparent in recent works [18–21] that smooth min-entropy is a relevant quantity for measuring quantum information. It is defined as²

$$H_{\min}^\epsilon(A|B)_\rho := \max_\lambda \{ \lambda \in \mathbb{R} \mid \exists \rho'_{AB} \in \mathcal{B}^\epsilon(\rho_{AB}), \sigma_B \in S_=(\mathcal{H}_B) \text{ s.t. } \rho'_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B \}. \quad (2)$$

The state σ_B is chosen from the set of normalized states $S_=(\mathcal{H}_B)$ in the Hilbert space \mathcal{H}_B . The state ρ'_{AB} is chosen from the set of subnormalized states in the Hilbert space \mathcal{H}_{AB} , that are also close to the state ρ_{AB} : $\mathcal{B}^\epsilon(\rho_{AB}) := \{ \rho'_{AB} \mid \rho'_{AB} \in S_=(\mathcal{H}_{AB}), P(\rho_{AB}, \rho'_{AB}) \leq \epsilon \}$. To specify this ϵ -ball around a state ρ , we use the purified distance $P(\rho, \sigma) := \sqrt{1 - F(\rho, \sigma)^2}$ (where $F(\rho, \sigma) := \|\sqrt{\rho}\sqrt{\sigma}\|_1$).³

3. DATA PROCESSING INEQUALITY

If the entropies are interpreted operationally then Theorem 1 deals with data processing in the one-shot scenario: a local physical operation is performed on a tripartite quantum system *once*, and a statement is made about the information content of such a system. Theorem 3 can be interpreted as an average scenario: a statement is made about the information content *on average*

¹ The Stinespring dilation allows for any completely positive trace preserving (CPTP) map to be decomposed into a unitary followed by a partial trace. Since the von Neumann entropy is invariant under unitaries, the DPI applies to any CPTP map applied to the system BC .

² It is sufficient to take the maximum over λ if a finite dimensional system is considered. However, in infinite dimensions it is necessary to take the supremum [22].

³ If ρ and σ are not normalized, then the generalized fidelity is used: $\bar{F}(\rho, \sigma) := \left\| \sqrt{\rho \oplus (1 - \text{Tr} \rho)} \sqrt{\sigma \oplus (1 - \text{Tr} \sigma)} \right\|_1$.

after applying a local physical operation to a tri-partite quantum state.

A. General Data Processing Inequality

Theorem 1 (Smooth min-entropy DPI).

Let $\rho \in S_=(\mathcal{H}_{ABC})$, then

$$H_{\min}^\epsilon(A|BC)_\rho \leq H_{\min}^\epsilon(A|B)_\rho. \quad (3)$$

Proof. First, we let $\lambda := H_{\min}^\epsilon(A|BC)_\rho$, and we choose the particular $\tilde{\rho}_{ABC} \in \mathcal{B}^\epsilon(\rho_{ABC})$ and σ_B in the definition of $H_{\min}^\epsilon(A|BC)_\rho$ such that λ is maximized. From Eqn. 2 we have $\tilde{\rho}_{ABC} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_{BC}$, and by tracing out system C we get: $\tilde{\rho}_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B$. We know that $\tilde{\rho}_{ABC} \in \mathcal{B}^\epsilon(\rho_{ABC})$, and therefore $P(\rho_{ABC}, \tilde{\rho}_{ABC}) \leq \epsilon$. Since the purified distance does not increase under the partial trace (see Lemma B.1), it follows that $P(\rho_{AB}, \tilde{\rho}_{AB}) \leq \epsilon$. Therefore we have $\tilde{\rho}_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})$, and $\sigma_B \in S_=(\mathcal{H}_B)$, which are candidates for maximizing $H_{\min}^\epsilon(A|B)_\rho$. \square

B. Specialized Data Processing Inequality

Now we have completed the proof of the DPI in the most general case, and the only remaining difficulty is to specialize Theorem 1 to the DPI for the von Neumann entropy. This specialization is achieved by using the limit of many i.i.d. copies of a state, called the QAEP [19].

Theorem 2 (QAEP).

Let $\rho \in S_=(\mathcal{H}_{AB})$ then

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\epsilon(A^n|B^n)_{\rho^{\otimes n}} = H(A|B)_\rho. \quad (4)$$

This directly reduces Theorem 1 to the DPI for the von Neumann entropy.

Theorem 3 (von Neumann entropy DPI).

Let $\rho \in S_=(\mathcal{H}_{ABC})$, then

$$H(A|BC)_\rho \leq H(A|B)_\rho. \quad (5)$$

However, in order to have a self contained proof of the data processing inequality for the von Neumann entropy we provide an alternative, shorter proof of the QAEP than that of [19].

4. QUANTUM ASYMPTOTIC EQUIPARTITION PROPERTY

In order to prove Theorem 2, we upper and lower bound $\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} H_{\min}^\epsilon(A^n|B^n)_{\rho^{\otimes n}}$ by $H(A|B)_\rho$. The lower bound (Lemma 4.1) is obtained by applying a chain rule to the conditional smooth min-entropy such that it is bounded by a difference of non-conditional smooth entropies. The i.i.d. limit of non-conditional smooth entropies can then be taken (Lemmas 5.2 and 5.3). The upper bound (Lemma 4.2) can

be obtained by bounding the smooth min entropy by the von Neumann entropy of a different state, and then using the continuity of the von Neumann entropy when the i.i.d. limit is taken (Lemma A.1).

For these proofs we will need the smooth 0th order Rényi entropy, which is defined as $H_0^\epsilon(A)_\rho := \min_{\rho' \in \mathcal{B}^\epsilon(\rho)} H_0(A)_{\rho'}$, where $H_0(A)_\rho := \log \text{rank} \rho$. In addition, we will need the non-conditional smooth min-entropy defined as $H_{\min}^\epsilon(A)_\rho := \max_{\rho' \in \mathcal{B}^\epsilon(\rho)} H_{\min}(A)_{\rho'}$, where $H_{\min}(A)_\rho := -\log \|\rho\|_\infty$. The infinity norm is defined as $\|\rho\|_\infty := \max_i \{|\lambda_i|\}$, where λ_i are the eigenvalues of ρ .

Lemma 4.1 (Lower bound on the conditional smooth min-entropy). Let $\rho_{AB} \in S_=(\mathcal{H}_{AB})$ then,

$$H(A|B)_\rho \leq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\epsilon(A^n|B^n)_{\rho^{\otimes n}}. \quad (6)$$

Proof. First we use the chain rule Lemma 5.1 applied to the state $\rho \in S_=(\mathcal{H}_{AB})$:

$$H_{\min}^{\frac{\epsilon}{3}}(AB)_\rho - H_0^{\frac{\epsilon}{3}}(B)_\rho \leq H_{\min}^\epsilon(A|B)_\rho. \quad (7)$$

We can apply Eqn. 7 to the state $\rho^{\otimes n}$, divide by n , and then take the limit as $\epsilon \rightarrow 0$ and $n \rightarrow \infty$. Using the non-conditional QAEP of Lemmas 5.2 and 5.3, we get

$$\begin{aligned} H(A|B)_\rho &\leq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} (H_{\min}^{\frac{\epsilon}{3}}(A^n|B^n)_{\rho^{\otimes n}} - \frac{1}{n} H_0^{\frac{\epsilon}{3}}(B^n)_{\rho^{\otimes n}}), \end{aligned} \quad (8)$$

where we use the definition of the conditional von Neumann entropy. \square

Lemma 4.2 (Upper bound on the conditional smooth min-entropy). Let $\rho_{AB} \in S_=(\mathcal{H})$ then,

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\epsilon(A|B)_\rho \leq H(A|B)_\rho. \quad (9)$$

Proof. First, we use Lemma 5.6 for the state $\rho_{A^n B^n}^{\otimes n}$:

$$H_{\min}^\epsilon(A^n|B^n)_{\rho^{\otimes n}} \leq H(A^n|B^n)_{\tilde{\rho}}, \quad (10)$$

where $\tilde{\rho} \in \mathcal{B}^\epsilon(\rho_{AB}^{\otimes n})$. Dividing by n , then taking the limit as $\epsilon \rightarrow 0$ and $n \rightarrow \infty$, and using Lemma A.1 we have:

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H(A^n|B^n)_{\tilde{\rho}} = H(A|B)_\rho. \quad (11)$$

\square

5. PROPERTIES OF SMOOTH ENTROPIES

The following are properties of smooth entropies used to prove Lemmas 4.1, and 4.2. In particular, we bound the smooth min-entropy and smooth 0th-order Rényi entropy in order to perform the i.i.d. limit of $\epsilon \rightarrow 0$, $n \rightarrow \infty$. For additional properties used in the following proofs, see the appendices.

Lemma 5.1 (Chain rule). *Let $\rho \in S_=(\mathcal{H}_{AB})$. Then*

$$H_{\min}^\epsilon(AB)_\rho - H_0^\epsilon(B)_\rho \leq H_{\min}^{3\epsilon}(A|B)_\rho. \quad (12)$$

Proof. First, we pick the particular $\rho'_{AB} \in \mathcal{B}^\epsilon(\rho_{AB})$ in the definition of the non-conditional smooth min-entropy $H_{\min}^\epsilon(AB)_\rho = \lambda$ such that it is maximized. We also pick the particular $\tilde{\rho}_B \in \mathcal{B}^\epsilon(\rho_B)$ from the definition of the 0th order Rényi entropy such that it is minimized, and write the projector onto its support as $\Pi := \Pi_{\text{supp}(\tilde{\rho}_B)}$. Now given that $\rho'_{AB} \leq 2^{-\lambda} \mathbb{1}_{AB}$, then $\Pi \rho'_{AB} \Pi \leq 2^{-\lambda} \mathbb{1}_A \otimes \mathbb{1}_{\text{supp}(\tilde{\rho}_B)}$, so we have

$$H_{\min}^\epsilon(AB)_\rho = \{\lambda | \Pi \rho'_{AB} \Pi \leq 2^{-\lambda} \mathbb{1}_A \otimes \mathbb{1}_{\text{supp}(\tilde{\rho}_B)}\}. \quad (13)$$

Now we will need to ensure that $\hat{\rho}_{AB} := \Pi \rho'_{AB} \Pi$ is close to ρ_{AB} . To do this, we use the triangle inequality for the purified distance (see Lemma 5 of [23]) in the first and third lines, as well as the fact that the purified distance decreases under the CP trace non-increasing map $\rho \rightarrow \Pi \rho \Pi$ (Lemma B.1) in the second line:

$$P(\hat{\rho}_{AB}, \rho_{AB}) \leq P(\hat{\rho}_{AB}, \tilde{\rho}_{AB}) + P(\tilde{\rho}_{AB}, \rho_{AB}) \quad (14)$$

$$\leq P(\rho'_{AB}, \tilde{\rho}_{AB}) + P(\tilde{\rho}_{AB}, \rho_{AB}) \quad (15)$$

$$\leq P(\rho'_{AB}, \rho_{AB}) + 2P(\tilde{\rho}_{AB}, \rho_{AB}) \quad (16)$$

$$= \epsilon + 2P(\tilde{\rho}_{AB}, \rho_{AB}), \quad (17)$$

where we purify $\tilde{\rho}_B$ to the state $|\phi\rangle_{ABC}$ and define $\tilde{\rho}_{AB} := \text{Tr}_C(|\phi\rangle\langle\phi|)$ (see Lemma 8 of [23]). Now all that is left to find is $P(\tilde{\rho}_{AB}, \rho_{AB})$. From Theorem 4 we have:

$$P(|\phi\rangle_{ABC}, |\psi\rangle_{ABC}) = P(\tilde{\rho}_B, \rho_B), \quad (18)$$

where $|\psi\rangle_{ABC}$ is chosen to be a purification of ρ_B such that $\text{Tr}_C|\psi\rangle\langle\psi| = \rho_{AB}$. Now since the purified distance doesn't increase under the partial trace (see Lemma B.1):

$$P(|\phi\rangle_{ABC}, |\psi\rangle_{ABC}) \leq P(\tilde{\rho}_{AB}, \rho_{AB}) \leq P(\tilde{\rho}_B, \rho_B). \quad (19)$$

Combining Eqns. 18, 19 we get

$$P(|\phi\rangle_{ABC}, |\psi\rangle_{ABC}) = P(\tilde{\rho}_{AB}, \rho_{AB}) = P(\tilde{\rho}_B, \rho_B). \quad (20)$$

We know that $P(\tilde{\rho}_B, \rho_B) \leq \epsilon$, and therefore $P(\tilde{\rho}_{AB}, \rho_{AB}) \leq \epsilon$. This makes Eqn. 17 $P(\hat{\rho}_{AB}, \rho_{AB}) \leq 3\epsilon$. Now returning to the smooth min-entropy in Eqn. 13, we define $\tau_{\tilde{\rho}_B} := \mathbb{1}_{\text{supp}(\tilde{\rho}_B)} / \text{rank}(\tilde{\rho}_B)$ so that we have

$$\begin{aligned} H_{\min}^\epsilon(AB)_\rho &= \{\lambda + \text{rank}(\tilde{\rho}_B) \mid \Pi \rho'_{AB} \Pi \leq 2^{-\lambda} \mathbb{1}_A \otimes \tau_{\tilde{\rho}_B}\} \\ &\leq \max_{\rho'' \in \mathcal{B}^{3\epsilon}(\rho)} \min_{\sigma_B} \{\lambda \mid \rho''_{AB} \leq 2^{-\lambda} \mathbb{1}_A \otimes \sigma_B\} + \log(\text{rank}(\tilde{\rho}_B)) \\ &= H_{\min}^{3\epsilon}(A|B)_{\rho_{AB}} + H_0^\epsilon(B)_{\rho_B}. \end{aligned} \quad (21)$$

□

Lemma 5.2 (Non-conditional QAEP for smooth min-entropy). *Let $\rho \in S_=(\mathcal{H}_A)$ then,*

$$H(A)_\rho \leq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\epsilon(A^n)_{\rho^{\otimes n}}. \quad (22)$$

Proof. First, we calculate the quantum Rényi entropy of order α , defined as $H_\alpha(A)_\rho := 1/(1-\alpha) \log \text{Tr} \rho^\alpha$ for the state $\rho^{\otimes n}$:

$$H_\alpha(A^n)_{\rho^{\otimes n}} = n H_\alpha(A)_\rho. \quad (23)$$

Now we may write Eqn. 26 from Lemma 5.4 as

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_{\min}^\epsilon(A^n)_{\rho^{\otimes n}} \geq H_\alpha(A)_\rho. \quad (24)$$

This is true for all $\alpha > 1$ and so in particular, it's true if we take the limit as $\alpha \rightarrow 1^+$, where we know from Lemma A.2 that $\lim_{\alpha \rightarrow 1} H_\alpha(A)_\rho = H(A)_\rho$. □

Lemma 5.3 (Non-conditional QAEP for 0th-order Rényi entropy). *Let $\rho \in S_=(\mathcal{H})$ then,*

$$H(A)_\rho \geq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H_0^\epsilon(A^n)_{\rho^{\otimes n}}. \quad (25)$$

Proof. This follows in a similar manner to the proof of Lemma 5.2, but now Lemma 5.5 is used. □

Lemma 5.4 (Lower bound on the smooth min-entropy). *Let $\rho \in S_=(\mathcal{H})$, and $\alpha > 1$, $\epsilon \in [0, 1]$ then*

$$H_\alpha(A)_\rho + \frac{\log(1 - \sqrt{1 - \epsilon^2})}{\alpha - 1} \leq H_{\min}^\epsilon(A)_\rho. \quad (26)$$

Proof. First, we let $\rho = \sum_x \lambda_x |x\rangle\langle x|$. We construct a quantum state σ whose eigenvectors are the same as ρ , and whose eigenvalues, ν_x , are $\nu_x = \lambda_x$ if $x \in \mathcal{X}$ and $\nu_x = 0$ otherwise, where $\mathcal{X} := \{x \in \{1, 2, \dots, \dim \mathcal{H}\} : \lambda_x \leq \lambda^*\}$, and $\lambda^* \in [0, 1]$. Hence $\sigma \in S_{\leq}(\mathcal{H})$. Now we may write the fidelity between ρ and σ as

$$\|\sqrt{\rho}\sqrt{\sigma}\|_1 = \sum_x \lambda_x^{1/2} \nu_x^{1/2} = \sum_{x \in \mathcal{X}} \lambda_x. \quad (27)$$

We can write (for $\alpha > 1$):

$$\sum_x \lambda_x^\alpha \geq \sum_{x \notin \mathcal{X}} \lambda_x^{\alpha-1} \lambda_x \geq \|\sigma\|_\infty^{(\alpha-1)} \sum_{x \notin \mathcal{X}} \lambda_x \quad (28)$$

$$= \|\sigma\|_\infty^{(\alpha-1)} (1 - F(\rho, \sigma)). \quad (29)$$

By taking the log of this equation and since $\nu_x \leq \|\sigma\|_\infty \forall x$ we get

$$H_\alpha(A)_\rho \leq \frac{1}{1-\alpha} \log(1 - F(\rho, \sigma)) + H_{\min}(A)_\sigma. \quad (30)$$

Now we choose a particular λ^* so that the fidelity is fixed to be $F(\rho, \sigma) = \sqrt{1 - \epsilon^2}$ ($1 \geq \epsilon > 0$). This means that $P(\rho, \sigma) \leq \epsilon$, and hence $\sigma \in \mathcal{B}^\epsilon(\rho)$, so $H_{\min}(A)_\sigma \leq H_{\min}^\epsilon(A)_\rho$. □

Lemma 5.5 (Upper bound on the 0th order Rényi entropy). *Let $\rho \in S_=(\mathcal{H})$, and $1/2 < \alpha < 1$ then*

$$H_0^\epsilon(A)_\rho \leq H_\alpha(A)_\rho + \frac{1}{\alpha - 1} \log \sqrt{1 - \epsilon}. \quad (31)$$

Proof. This proof follows similarly to the proof of Lemma 5.4. We can construct a quantum state σ in the same manner as Lemma 5.4. Now $1/2 < \alpha < 1$ so we have $\sum_x \lambda_x^\alpha \geq \sum_{x \in \mathcal{X}} \lambda_x^\alpha \geq (1/\text{rank} \sigma)^{(\alpha-1)} \sum_{x \in \mathcal{X}} \lambda_x$. Taking the log gives $H_\alpha(A)_\rho \geq \frac{1}{1-\alpha} \log F(\rho, \sigma) + H_0(A)_\sigma$. Now we choose a particular λ^* so that we can write the fidelity as $F(\rho, \sigma) = \sqrt{1-\epsilon}$, ($1 \geq \epsilon > 0$), and so $\sigma \in \mathcal{B}^\epsilon(\rho)$. Then $H_0(A)_\sigma \geq H_0^\epsilon(A)_\rho$, which gives the result. \square

Lemma 5.6 (Relation of conditional von Neumann entropy and conditional smooth min-entropy). *Let $\rho \in S_=(\mathcal{H})$, then $\exists \tilde{\rho} \in \mathcal{B}^\epsilon(\rho)$ such that*

$$H_{\min}^\epsilon(A|B)_\rho \leq H(A|B)_{\tilde{\rho}}. \quad (32)$$

Proof. We start with the definition of the conditional von Neumann entropy for subnormalized states $\tilde{\rho}_{AB} \in S_{\leq}(\mathcal{H}_{AB})$, so we have

$$H(A|B)_{\tilde{\rho}} := \frac{1}{\text{Tr} \tilde{\rho}_{AB}} \max_{\sigma_B} \text{Tr}(\tilde{\rho}_{AB}(\log(\mathbb{1}_A \otimes \sigma_B) - \log(\tilde{\rho}_{AB}))) \geq \frac{1}{\text{Tr} \tilde{\rho}_{AB}} \text{Tr}(\tilde{\rho}_{AB}(\log(\lambda \mathbb{1}_A \otimes \sigma'_B) - \log(\tilde{\rho}_{AB}))) - \log \lambda,$$

where we drop the maximization, picking a specific σ'_B : the state that allows λ to be maximized in $H_{\min}(A|B)_\rho$. We have also added and subtracted $\log \lambda$, defined as $-\log \lambda = H_{\min}^\epsilon(A|B)_\rho$, and we choose $\tilde{\rho}$ to be the state that allows λ to be maximized in the definition of $H_{\min}^\epsilon(A|B)_\rho$. Also, to simplify our expression, we use the quantum relative entropy, defined as $H(\rho||\sigma) :=$

$\text{Tr}(\rho \log \rho) - \text{Tr}(\rho \log \sigma)$. Now we may write

$$-\frac{1}{\text{Tr} \tilde{\rho}_{AB}} H(\tilde{\rho}_{AB} || \lambda \mathbb{1}_A \otimes \sigma'_B) + H_{\min}^\epsilon(A|B)_\rho \geq H_{\min}^\epsilon(A|B)_\rho,$$

where in the last line, we use the monotonicity of the log to show that $\tilde{\rho}_{AB} \log \tilde{\rho}_{AB} \leq \tilde{\rho}_{AB} \log(\lambda \mathbb{1}_A \otimes \sigma'_B)$. This then implies $-H(\tilde{\rho}_{AB} || \lambda \mathbb{1}_A \otimes \sigma'_B) \geq 0$. \square

6. ACKNOWLEDGEMENTS

The authors acknowledge support from the European Research Council (grant no. 258932), and the Swiss National Science Foundation (grant no. 200020-135048).

-
- [1] Michael A Nielsen and I Chuang. *Quantum Computation and Quantum Information*. Cambridge University Press, 2000.
 - [2] John Von Neumann. *Mathematische Grundlagen der Quantenmechanik*. Berlin: Springer, 1955.
 - [3] Elliott H. Lieb. Convex Trace Functions and the Wigner-Yanase-Dyson Conjecture. *Adv. Math.*, 11:267–288, 1973.
 - [4] Elliott H. Lieb and Mary B. Ruskai. Proof of the Strong Subadditivity of Quantum Mechanical Entropy. *J. Math. Phys.*, 14:1938–1941, 1973.
 - [5] Barry Simon. *Trace Ideals and Their Applications*. Cambridge University Press, Cambridge, 1979.
 - [6] Michael A. Nielsen and Denes Petz. A Simple Proof of the Strong Subadditivity Inequality. *Quantum Information and Computation*, 5(6):517–513, 2005.
 - [7] Dénes Petz. Quasi-Entropies for Finite Quantum Systems. *Reports on Mathematical Physics*, 23:57–65, 1984.
 - [8] M. B. Ruskai. Another Short and Elementary Proof of Strong Subadditivity of Quantum Entropy. *Reports on Mathematical Physics*, 60:1–12, 2007.
 - [9] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Quantum State Merging and Negative Information. *Communications in Mathematical Physics*, 269(1):107–136, October 2006.
 - [10] Michał Horodecki, Jonathan Oppenheim, and Andreas Winter. Partial Quantum Information. *Nature*, 436(7051):673–6, August 2005.
 - [11] Eric A. Carlen and Elliott H. Lieb. A Minkowski Type Trace Inequality and Strong Subadditivity of Quantum Entropy. *American Mathematical Society Translations*, 189(2):59–69, January 1999.
 - [12] Eric A. Carlen and Elliott H. Lieb. A Minkowski Type Trace Inequality and Strong Subadditivity of Quantum Entropy II: Convexity and Concavity. *Lett. Math. Phys.*, 83(2):107–126, 2008.
 - [13] Matthew Headrick and Tadashi Takayanagi. A Holographic Proof of the Strong Subadditivity of Entanglement Entropy. *Physical Review D*, 76(10):9, November 2007.
 - [14] Tomoyoshi Hirata and Tadashi Takayanagi. AdS/CFT and Strong Subadditivity of Entanglement Entropy. *Journal of High Energy Physics*, 2007(02):042–042, February 2007.
 - [15] Patrick Hayden, Richard Jozsa, Denes Petz, and Andreas Winter. Structure of States which Satisfy Strong Subadditivity of Quantum Entropy with Equality. *Commun. Math. Phys.*, 246(2):359–374, 2004.

- [16] Fedor Herbut. On Mutual Information in Multipartite Quantum States and Equality in Strong Subadditivity of Entropy. *J. Phys. A: Math. Gen.*, 37:3535–3542, 2004.
- [17] Anna Jencova and Mary Beth Ruskai. A Unified Treatment of Convexity of Relative Entropy and Related Trace Functions, with Conditions for Equality. *Rev. Math. Phys.*, 22(9):1099–1121, March 2010.
- [18] Robert König, Renato Renner, and Christian Schaffner. The Operational Meaning of Min- and Max-Entropy. *IEEE Trans. on Inf. Theory*, 55(9):4337–4347, 2009.
- [19] Marco Tomamichel, Roger Colbeck, and Renato Renner. A Fully Quantum Asymptotic Equipartition Property. *IEEE Trans. on Inf. Theory*, 55(12):5840–5847, 2009.
- [20] Nilanjana Datta. Min- and Max- Relative Entropies and a New Entanglement Monotone. pages 2816–2826, March 2008.
- [21] Renato Renner. *Security of Quantum Key Distribution*. Phd thesis, ETH Zürich, 2005.
- [22] Fabian Furrer, Johan Aberg, and Renato Renner. Min- and Max-Entropy in Infinite Dimensions. *arXiv:1004.1386*, (to appear in Comm. Math. Phys.) April 2010.
- [23] Marco Tomamichel, Roger Colbeck, and Renato Renner. Duality Between Smooth Min- and Max-Entropies. 2009.
- [24] Thomas M. Cover and Joy A. Thomas. *Elements of Information Theory*. Wiley, 1991.
- [25] Mario Berta, Matthias Christandl, Roger Colbeck, Joseph M. Renes, and Renato Renner. The Uncertainty Principle in the Presence of Quantum Memory. *Nature Physics*, 6(9):659–662, July 2010.
- [26] Christopher A. Fuchs and Jeroen van de Graaf. Cryptographic distinguishability measures for quantum-mechanical states. *IEEE Trans. Inf. Theory*, 45(4):1216–1227, 1999.
- [27] Mark Fannes. A Continuity Property of the Entropy Density for Spin Lattice Systems. *Commun. Math. Phys.*, 31:291–294, 1973.
- [28] Armin Uhlmann. The ‘Transition Probability’ in the State Space of a *-Algebra. *Reports on Mathematical Physics*, 9(2):273–279, September 1976.

Appendix A: Known Entropic Properties

The following are known properties used in the proof of Theorem 2, which we include here for completeness.

Lemma A.1 (Limit of the conditional von Neumann entropy of an almost i.i.d. state). *Let $\rho \in S_=(\mathcal{H})$ and $\sigma_n \in \mathcal{B}^\epsilon(\rho^{\otimes n})$, then*

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} H(A^n | B^n)_{\sigma_n} = H(A|B)_\rho. \quad (\text{A-1})$$

Proof. First, we know that $\sigma_n \in \mathcal{B}^\epsilon(\rho^{\otimes n})$, and by Eqn. 20 we have $P(\rho_B^{\otimes n}, \sigma_{n_B}) \leq \epsilon$. Now we show Eqn. A-1 is valid when the system B is trivial, i.e. $H(A^n | B^n)_{\sigma_n} = H(A^n)_{\sigma_n}$ and $H(A|B)_\rho = H(A)_\rho$ (see Chapter 3 of [24]).

First, we extend $\rho_A^{\otimes n}$ and σ_{n_A} to $\rho'_n := \rho_A^{\otimes n} \oplus 0$ and $\sigma'_n := \sigma_{n_A} \oplus (1 - \text{Tr} \sigma_{n_A})$ so that $\sigma'_n \in S_=(\mathcal{H}_A \oplus \mathcal{H}_1)$ (where \mathcal{H}_1 is a one dimensional space). Next, we define the state $\tilde{\sigma}_n := \sum_i s'_i |i\rangle\langle i|$, where s'_i are the eigenvalues of σ'_n ordered such that $s'_i \geq s'_{i+1}, \forall i$ and $|i\rangle$ are the eigenvectors of ρ'_n . It is clear that $P(\rho_A^{\otimes n}, \sigma_{n_A}) = P(\rho'_n, \sigma'_n)$, and so by

Lemma A.4 of [25], we know that $P(\rho'_n, \sigma'_n) \geq P(\rho'_n, \tilde{\sigma}_n)$. The purified distance is lower bounded by the trace distance, and so $P(\rho'_n, \tilde{\sigma}_n) \geq D(\rho'_n, \tilde{\sigma}_n)$ (see [26]). Now since $\sigma_{n_A} \in \mathcal{B}^\epsilon(\rho_A^{\otimes n})$ we know $D(\rho'_n, \tilde{\sigma}_n) \leq \epsilon$. Now we may use Fanne’s Inequality [27]:

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} |H(A^n)_{\tilde{\sigma}_n} - H(A^n)_{\rho'_n}| \quad (\text{A-2})$$

$$\leq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} (\epsilon \log d^n + \eta(\epsilon)) = 0, \quad (\text{A-3})$$

where we define $\eta(x) := -x \log x$, and $d = \dim(\mathcal{H})$. This is not the limit we would like to know, so we compare the entropies here to those of Eqn. A-1 for trivial B . From the definition of $\tilde{\sigma}_n$ we know that $H(A^n)_{\tilde{\sigma}_n} = H(A^n)_{\sigma_n} - \eta(1 - \text{Tr} \sigma_n)$ and so

$$\lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} |H(A^n)_{\rho^{\otimes n}} - H(A^n)_{\sigma_n}| \quad (\text{A-4})$$

$$\leq \lim_{\epsilon \rightarrow 0} \lim_{n \rightarrow \infty} \frac{1}{n} (|H(A^n)_{\rho'_n} - H(A^n)_{\tilde{\sigma}_n}| + |\eta(1 - \text{Tr} \sigma_n)|) = 0,$$

where we know that $0 \leq (1 - \text{Tr} \sigma_{n_A}) \leq 1$, and hence $0 \leq \eta(1 - \text{Tr} \sigma_{n_A}) \leq 1/2$.

When B is non-trivial we can combine Eqn. A-4 with Eqn. 23 and the definition of the conditional von Neumann entropy to get the result. \square

Lemma A.2 (Relation of Rényi entropy and von Neumann entropy). *Let $\rho \in S_=(\mathcal{H})$ then,*

$$\lim_{\alpha \rightarrow 1} H_\alpha(A)_\rho = H(A)_\rho. \quad (\text{A-5})$$

Proof. See [24]. \square

Appendix B: Known Distance Properties

Theorem 4 (Uhlmann’s Theorem). *Given $\rho, \sigma \in S_=(\mathcal{H})$ then*

$$F(\rho, \sigma) = \max_{|\psi\rangle, |\phi\rangle} |\langle \psi | \phi \rangle| = \max_{|\phi\rangle} |\langle \psi | \phi \rangle|, \quad (\text{A-1})$$

where $|\phi\rangle, |\psi\rangle$ are purifications of ρ and σ respectively.

Proof. See Theorem 9.4 in [1] or [28]. \square

Lemma B.1 (Purified distance under CP trace non-increasing maps). *Let \mathcal{E} be a trace non-increasing map, and $\rho, \sigma \in S_=(\mathcal{H})$ then,*

$$P(\mathcal{E}(\rho), \mathcal{E}(\sigma)) \leq P(\rho, \sigma). \quad (\text{A-2})$$

This can be proven by using the fact that the fidelity cannot decrease under completely positive trace non-increasing maps.

Proof. See Lemma 7 of [23]. \square